IN THE CLAIMS:

Please amend claims 1-8, 11-12, 15, 20, 25-26, 30-35, 38 and 41 as indicated below.

Please add new claims 42-61 as indicated below.

This listing of claims below will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) ~~Method~~ A method for proving the pedigree and/or for the identification of animals or organisms or of biological material from animals and organisms, which comprises the following steps:

providing genetic information of an animal, an organism or biological material of an animal or organism unambiguously identifying the animal or organism or the biological material,

storing on a data carrier, not necessarily attached to the animal or organism or to the biological material, identification data in the form of a message which has been encrypted by a symmetric or asymmetric key and which has an unambiguous and predetermined ~~connection with~~ verifiable relation to said genetic information unambiguously identifying ~~an~~ the animal or the biological material, and

verifying the identification data with respect to whether said data have the predetermined ~~connection with~~ verifiable relation to the genetic information.

2. (Currently Amended) Method according to claim 1 further comprising the step of storing predetermined genetic information of one or more animals or organisms or of biological material from one or more animals or organisms as reference datasets on a storage medium.

3. (Currently Amended) Method according to Claim 1 wherein the data carrier holds further data which have been assigned to the identification data and which relate to the animal or organism to be identified or the biological material to be identified.

4. (Currently Amended) Method according to claim 1 wherein the identification data contain an encrypted message which has been encrypted using a code unambiguously assigned to the individual animal, organism or biological material.

5. (Currently Amended) Method according to Claim 4, wherein the encrypted message contains the value of a one-way function (hash), which value is obtained when applying said one-way function to further data which are stored on the data carrier and which relate to the animal or organism to be identified or the biological material to be identified.

6. (Currently Amended) Method according to claim 1 wherein an encrypted message comprises genetic information unambiguously identifying the animal, the organism or the biological material.

7. (Currently Amended) Method according to claim 3 wherein the identification data comprise encrypted data which relate to the storage location and/or the contents of further data which relate to the animal, the organism or the biological material assigned to the identification data.

8. (Currently Amended) Method according to claim 4 wherein the identification data comprise a message encrypted by a code which is generated in a predetermined unambiguous manner on the basis of a sequence of digits which has been unambiguously assigned to genetic information unambiguously identifying the animal, the organism or the biological material.

9. (Previously Presented) Method according to Claim 8, wherein the sequence of digits forms at least part of the code.

10. (Previously Presented) Method according to Claim 4 wherein the message has been encrypted using a symmetric key.

11. (Currently Amended) Method according to Claim 4 wherein the message has been encrypted on the basis of the private key of an asymmetric pair of keys, with the public key

at least in part having a predetermined relationship to the genetic information identifying the animal, the organism or the biological material.

12. (Currently Amended) Method according to claim 11 wherein the public key comprises a part specific for the animal, the organism or the biological material and a user-specific part.

13. (Previously Presented) Method according to claim 8 wherein the identification data are additionally encrypted using a user-specific key.

14. (Previously Presented) Method according to claim 4 wherein the data on the data carrier, which have been assigned to the identification data, have at least in part been encrypted by a code which is different than the code used for encrypting the identification data.

15. (Currently Amended) Method according to claim 4 wherein ~~the key~~ a key for decrypting the message contained in the identification data is stored on a carrier of a chip for communicating with a data processing system via an interface, in particular on a smartcard.

16. (Previously Presented) Method according to Claim 15, wherein the chip has a device for decrypting messages.

17. (Previously Presented) Method according to Claim 15 wherein the key encoding the message of the identification data is an asymmetric key, the corresponding private key is stored on the chip and the chip has a device for encrypting messages using the private key.

18. (Previously Presented) Method according to claim 15 wherein the chip contains an interface for entering digitized genetic information and a device for verifying the assignment of the stored code to entered digitized genetic information.

19. (Previously Presented) Method according to claim 18 wherein the verifying device compares the entered digitized genetic information with a stored value for this information and emits an output signal which indicates whether or not there is a match.

20. (Currently Amended) Method according to Claim 18, wherein, based on the entered digitized genetic information and a stored assignment to the stored key of digitized genetic information unambiguously identifying the animal, the organism or the biological material, the verifying device determines a key assigned to the entered information, compares the key determined in this way with the stored key and releases an output signal which indicates whether or not the key determined based on the input matches the stored key.

21. (Previously Presented) Method according to claim 15 wherein the chip holds information identifying one or more users and the decrypting device or encrypting device is only activated when information stored for identifying a user is entered via an input device.

22. (Previously Presented) Method according to claim 4 wherein the code for decrypting coded information contained in the identification data is stored on a central computer.

23. (Previously Presented) Method according to Claim 22, wherein the computer determines the corresponding key owing to entered or predetermined genetic information and applies said key to the identification data.

24. (Previously Presented) Method according to Claim 23, wherein, after decrypting, the central computer verifies whether predetermined sequences of characters are present in the decrypted text and releases a corresponding output signal to a user.

25. (Currently Amended) Method according to Claim 23 wherein the information stored on the data carrier and, where appropriate, predetermined genetic information unambiguously identifying the animal, the organism or the biological material are transferred to the central computer.

26. (Currently Amended) Method according to claim 1 wherein the data carrier containing the data related to the animal, the organism or the biological material comprises a portion of a central computer.

27. (Previously Presented) Method according to Claim 26, wherein at least in part the data are access-protected and that access authorization is different for different users of the central computer.

28. (Previously Presented) Method according to Claim 26, wherein a proportion of users can access at least part of the stored data only, if a predetermined further user is logged on to the central computer at the same time.

29. (Previously Presented) Method according to claim 26, wherein access to at least part of the stored data is only possible, if the computer has verified access authorization using the data stored on a chip, in particular on a smartcard.

30. (Currently Amended) Method according to claim 26, wherein the computer is set up such that users can write to the stored data related to the animal, the organism or the biological material only together with a digital signature of the user.

31. (Currently Amended) Method according to claim 26 wherein ~~an animal-specific~~ a pair of asymmetric keys specific to the animal, the organism or the biological material is used for exchanging a session key for communication of a user with the central computer.

32. (Currently Amended) ~~Method~~ A method for generating data which are unambiguously and verifiably ~~connected with~~ related to an individual animal or organism or to biological material from an animal or organism, which comprises:

providing genetic information of an animal, an organism or biological material of an animal or organism unambiguously identifying the animal or organism or the biological material,

creating identification data in the form of a message which has been encrypted by a symmetric or asymmetric key and which has an unambiguous and predetermined ~~connection~~

~~with~~ verifiable relation to genetic information which unambiguously identifies an animal, an organism or the biological material, and

storing the identification data on a data carrier not necessarily attached to the animal, the organism or to the biological material from the animal or organism.

33. (Currently Amended) Method according to Claim 32, wherein the identification data contain an encrypted message which has been encrypted using a key unambiguously assigned to the individual animal, organism or biological material.

34. (Currently Amended) Method according to Claim 33, wherein the encrypted message contains the value of a one-way function (hash), which value is obtained when applying said one-way function to further data which are stored on the data carrier and which relate to the animal or organism to be identified or the biological material to be identified.

35. (Currently Amended) Method according to claim 32 wherein the identification data comprise a message encrypted by a code which is generated in a predetermined unambiguous manner on the basis of a sequence of digits which has been unambiguously assigned to genetic information unambiguously identifying the animal, the organism or the biological material.

36. (Previously Presented) Method according to Claim 35, wherein the key is a symmetric key.

37. (Previously Presented) Method according to Claim 35, wherein the information has been encrypted on the basis of an asymmetric pair of keys, with the public key at least in part having a predetermined relationship to the genetic information.

38. (Currently Amended) ~~Chip~~ A chip carrier for identifying ~~animals~~ an animal or biological material from an animal, said chip carrier being set up for communication between a chip on the chip carrier, which is not necessarily attached to the animal or to the biological material from the animal, and a computer via an interface, in particular a smartcard, wherein the

chip holds a key which has an unambiguous and predetermined ~~connection with~~ verifiable relation to genetic information specific for the individual animal, organism or biological material from the animal or organism.

39. (Previously Presented) Chip carrier according to Claim 38, wherein the chip has a processor for decrypting messages using the stored key.

40. (Previously Presented) Chip carrier according to claim 38 wherein the chip contains an interface for entering digitized genetic information and a device for verifying the assignment of the stored code to entered digitized genetic information.

41. (Currently Amended) ~~Computer~~ A computer system for carrying out a method according to claim 1 comprising a central computer having a data carrier which holds identification data which have an unambiguous and predetermined ~~connection with~~ verifiable relation to genetic information unambiguously identifying an animal, an organism or ~~the~~ biological material from an animal or organism.

42. (New) Method according to claim 4 wherein the code is generated at least in part based upon the genetic information of the individual animal, organism or biological material.

43. (New) Method according to claim 33, wherein the key is generated at least in part based upon the genetic information of the individual animal, organism or biological material.

44. (New) A digital certificate for unambiguously identifying an animal, an organism or biological material of an animal or organism, comprising

an identifying genetic information or genetic identification data that is unambiguously related to genetic information, the identifying genetic information or genetic identification data uniquely identifying the animal, the organism or the biological material, and

a digital signature of a certification authority authenticating the genetic information or genetic identification data.

45. (New) The digital certificate according to claim 44, further comprising one of more data or information chosen from the group consisting of a photographic picture, pedigree data, specific skills, ownership data, prizes and awards, value declarations, training, biological information, birth data, genetic or other diseases, vaccination history, veterinary visit information and diagnostic test results, and wherein said digital signature authenticates the one of more data or information.

46. (New) The digital certificate according to claim 44, wherein the genetic information or genetic identification data have been encrypted using a key or code unambiguously assigned to an individual animal, an individual organism or the biological material of an individual animal or organism.

47. (New) The digital certificate according to claim 46, wherein the key or code comprises a symmetric key.

48. (New) The digital certificate according to claim 47, further comprising said symmetric key.

49. (New) The digital certificate according to claim 47, wherein said symmetric key pair is uniquely assigned to the animal, the organism or the biological material.

50. (New) The digital certificate according to claim 47, wherein said symmetric key pair is generated at least in part based upon the genetic information identifying the animal, the organism or the biological material.

51. (New) The digital certificate according to claim 46, wherein the key or code comprises a private key of an asymmetric key pair.

52. (New) The digital certificate according to claim 51, further comprising a public key of said asymmetric key pair.

53. (New) The digital certificate according to claim 51, wherein said asymmetric key pair is uniquely assigned to the animal, the organism or the biological material.

54. (New) The digital certificate according to claim 51, wherein said asymmetric key pair has, at least in part, a predetermined relationship to the genetic information identifying the animal, the organism or the biological material.

55. (New) The digital certificate according to claim 54, wherein said asymmetric key pair is generated at least in part based upon the genetic information identifying the animal, the organism or the biological material.

56. (New) The digital certificate according to claim 44, wherein said identifying genetic information uniquely identifies the animal, the organism or the biological material, and said genetic identification data is derived as a result of a mathematical function being applied to said identifying genetic information.

57. (New) A method for unambiguously identifying an animal, an organism or biological material of an animal or organism by means of a digital certificate, the digital certificate comprising identification data having an unambiguous and predetermined relation to genetic information unambiguously identifying the animal or biological material, and a digital signature of a certification authority, the method comprising

reading said identification data and said digital signature from said digital certificate,

comparing said identification data on said digital certificate with independently obtained identification data for said animal, organism or biological material, and

verifying that the independently obtained identification data have the predetermined relation to said genetic information.

58. (New) The method according to claim 57, wherein the certificate comprises a key uniquely assigned to the specific animal, organism or biological material and said identification data is in the form of a message that has been encrypted using said key.

59. (New) The method according to claim 58, wherein said key is generated at least in part based upon the genetic information data identifying the animal, the organism or the biological material.

60. (New) The method according to claim 58, wherein said key is a public key of an asymmetric key pair, and encryption of said message was done by means of a private key of said asymmetric key pair.

61. (New) The method according to claim 58, wherein said key comprises a symmetric key.